The effect of multi-pair signal states in quantum cryptography with entangled photons

Miloslav Dušek[1] and Kamil Brádler[2]

[1] *Department of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Republic*

[2] *Department of Chemical Physics and Optics, Charles University, Ke Karlovu 3, 121 16 Prague 2, Czech Republic*

(February 1, 2008)

Real sources of entangled photon pairs (like parametric down conversion) are not perfect. They produce quantum states that contain more than only one photon pair with some probability. In this paper it is discussed what happens if such states are used for the purpose of quantum key distribution. It is shown that the presence of "multi-pair" signals (together with low detection efficiencies) causes errors in transmission even if there is no eavesdropper. Moreover, it is shown that even the eavesdropping, that draws information only from these "multi-pair" signals, increases the error rate. Information, that can be obtained by an eavesdropper from these signals, is calculated.

03.67.Dd, 03.67.Hk, 03.65.Bz, 42.79.Sz

I. INTRODUCTION

The only evincibly secure method of communication with guaranteed privacy is Vernam cipher (or one-time pad) [1]. It requires both communicating parties share a secret key of the same length as the message. Quantum key distribution (QKD) is a technique to provide two parties with such a secure, secret and shared key. The first complete protocol for QKD was given by Bennett and Brassard [2] (BB84) following Wiesner's ideas [3]. The essence of this protocol is that if non-orthogonal quantum states are used for communication and a channel transmit them perfectly then eavesdropping is detectable. Later a different protocol, inspired by Bell's inequalities, was proposed by Ekert [4]. It relies on nonclassical correlations or entanglement of two quantum particles. Its simplified ("BB84-like") version works as follows: Let us suppose two communicating parties, *Alice* and *Bob*, share a set of entangled pairs $(|V\rangle_A |V\rangle_B + |H\rangle_A |H\rangle_B)/\sqrt{2}$, where $|V\rangle$ and $|H\rangle$ are two orthonormal states of each particle – e.g., vertical and horizontal linear polarizations of photons. Alice and Bob choose randomly and independently between two conjugated polarization bases – e.g. between basis $\{V, H\}$ ("+") and the "diagonal" basis ("×") rotated by 45° with respect to it. Following a public discussion about the basis of the measurement apparatuses, Alice and Bob can obtain a shared key made up from those signals where the measurement devices give correlated results. This is so called sifted key.

Photon pairs with correlated polarizations can be prepared, e.g., by parametric down conversion of type II [5] or using two down-conversion crystals with phase matching of type I [6]. Unfortunately, these techniques never produce exactly one pair of photons. Quantum states generated by the both above mentioned down-conversion methods should be the same in principle. However, the system with two non-linear crystals is perhaps more graphical for our purposes. The orientation of the optical axes of two identical crystals are mutually perpendicular. With a vertically (horizontally) polarized pump beam down-conversion will only occur in the first (second) crystal, respectively. A 45°-polarized pump photon will be equally likely to down-convert in either crystal. Let us suppose two spatial modes with two fixed frequencies fulfilling phase-matching conditions. One is aiming to Alice, the other to Bob. The first crystal generates beams with vertical polarizations, the second one with horizontal polarizations. Quantum state generated by one crystal can be described [7] as[1]

$$|\psi\rangle = \xi \sum_{n=0}^{\infty} g^n |n\rangle_A |n\rangle_B \,, \tag{1}$$

where $|n\rangle$ are corresponding number states, $\xi = (\cosh \chi t)^{-1} = \sqrt{1-g^2}$, and $g = \tanh \chi t$ with χ being proportional to non-linear susceptibility and pump power and t being interaction time.[2] The total quantum state originating from the both crystals is then[3]

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle_1 |\psi\rangle_2 \\ &= \xi^2 \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} g^{m+n} |m\rangle_{AV} |m\rangle_{BV} |n\rangle_{AH} |n\rangle_{BH} \,, \end{aligned} \tag{2}$$

where the subscripts V and H denote modes with vertical polarization (produced by the first crystal) and horizontal polarization (coming from the second crystal), respectively. The mean number of pairs is

$$\mu = \xi^4 \sum_{m,n} (m+n) g^{2(m+n)} = \frac{2g^2}{1-g^2}. \tag{3}$$

[1] Of course, this is just an approximation because more then only two modes are always present in real cases. If the number of signal or idler modes is effectively infinite then the total number of photons in signal or idler beam, respectively, obeys Poissonian statistics.

[2] It has good physical meaning only for pulse-pumped down conversion. Then it may be limited to infinity.

[3] We neglect a slight decrease of the pump power behind the first crystal.

The presence of more than one pair (or more than one photon in "single-photon" protocols) in the signals may enable eavesdropper (*Eve*) to get some information on the cryptographic key without causing any error. Thus she can learn something about the key but stay undisclosed. Similar difficulties implied by the use of weak coherent states in combination with lossy lines has been pointed out earlier [8–11]. A comprehensive analysis of security aspect of practical quantum cryptosystems taking into account the source imperfections were done in Ref. [12]. But the role of down-conversion sources was reduced just to the preparation of approximate single photon states there. In the present paper we want to go beyond this limitation.

The article is organized as follows. In Sec. II we explain, on a simplified signal state containing at most two pairs of photons, why errors appear in QKD. Imperfect detection efficiency and losses on the line are taken into account. Sec. III contains the comparison of the amount of information that can be obtained by Eve from multi-pair or multi-particle signals (by means of photon-number-splitting attack [12]) for different cryptographic schemes. Particularly for quantum cryptography using entangled photons, weak coherent states, and down-conversion "single-photon" sources. In Sec. IV we briefly discuss restrictions on Eve's activity stemming from monitoring both the data rate and the "double-click" rate (both detectors corresponding to logical 1 and 0 fire together). Sec. V concludes the article with a short summary.

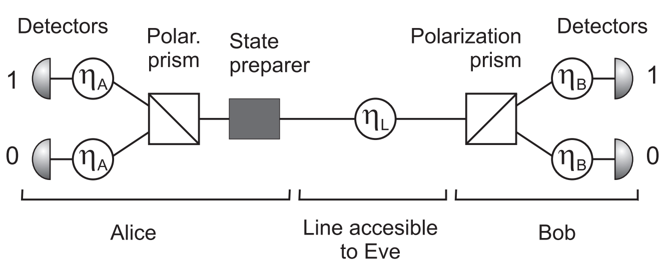

FIG. 1. Arrangement for QKD. State preparer, situated at Alice's side, generates signal states (2). Both Alice and Bob have detectors that cannot distinguish the number of impinging photons and whose detection efficiencies are η_A and η_B, respectively (this is indicated by circles in the figure). Alice and Bob change between two orientations of their polarization analyzers: $+$ and $\times$. Both communicating parties are connected by quantum channel with transmittance η_L. This channel is accessible to Eve.

II. ERRORS IN QKD DUE TO IMPERFECT SIGNAL STATES

Consider configuration for QKD as in Fig. 1. Let us suppose that $g \ll 1$ so that in Eq. (2) we can neglect all terms containing more than two pairs:

$$|\Psi\rangle = \xi\big[\,|0,0,0,0\rangle + g\big(\,|0,0,1,1\rangle + |1,1,0,0\rangle\,\big) + g^2\big(\,|0,0,2,2\rangle + |2,2,0,0\rangle + |1,1,1,1\rangle\,\big) + \mathcal{O}(g^3)\big]. \quad (4)$$

Here we have used notation

$$|m,m,n,n\rangle = |m\rangle_{AV}\,|m\rangle_{BV}\,|n\rangle_{AH}\,|n\rangle_{BH} = \frac{1}{m!n!}\left[\left(\mathsf{a}^\dagger_{AV}\mathsf{a}^\dagger_{BV}\right)^m\left(\mathsf{a}^\dagger_{AH}\mathsf{a}^\dagger_{BH}\right)^n\right]|\mathrm{vac}\rangle \quad (5)$$

with $\mathsf{a}^\dagger$ being creation operators in corresponding modes.

In the diagonal basis $\times$, represented by the following creation operators

$$\begin{aligned}\mathsf{a}^\dagger_X &= (\mathsf{a}^\dagger_V + \mathsf{a}^\dagger_H)/\sqrt{2},\\ \mathsf{a}^\dagger_Y &= (\mathsf{a}^\dagger_V - \mathsf{a}^\dagger_H)/\sqrt{2},\end{aligned} \quad (6)$$

state (4) does *not change* its form. It can be shown that even the full state (2) is invariant under such transformations of bases (the same transformation at the both sides).

Losses on the channel and non-perfect efficiency of Alice's and Bob's detectors are modeled by beam splitters with intensity transmittances η_L, η_A, and η_B, respectively. All the detectors are assumed to be "yes/no" detectors, which either fire or do not fire – they cannot distinguish the number of impinging photons. They may be described by the pair of projectors: $\mathsf{P}_{\mathrm{no}} = |0\rangle\langle 0| + \sum_{n=1}^{\infty}(1-\eta)^n|n\rangle\langle n|$ and $\mathsf{P}_{\mathrm{yes}} = \sum_{n=1}^{\infty}[1-(1-\eta)^n]|n\rangle\langle n|$, where η is a detector efficiency. We neglect any noise.

We intend to show that if the detector efficiencies are lower than 100 % the use of signal states (4) causes errors in the sifted key inevitably. Therefore we are interested only in that cases when Alice and Bob have set the same polarization bases. Of course, Alice and Bob include to the key only that events when *exactly one* detector fires at each side. The average relative length of the sifted key (with respect to the number of all generated entangled states) is then given by the formula[4]

$$\begin{aligned}R_{\mathrm{key}} \approx \xi^2 g^2\big\{&\eta_A\eta_B\eta_L\\ &+ g^2\left[1-(1-\eta_A)^2\right]\left[1-(1-\eta_B\eta_L)^2\right]\\ &+ 2g^2\eta_A(1-\eta_A)\,\eta_B\eta_L(1-\eta_B\eta_L)\big\}.\end{aligned} \quad (7)$$

On the other hand, the relative number of errors (i.e. events when Alice gets a bit different from that detected by Bob) is

$$R_{\mathrm{err}} \approx \xi^2 g^4\eta_A(1-\eta_A)\,\eta_B\eta_L(1-\eta_B\eta_L). \quad (8)$$

Thus the error rate reads

$$\begin{aligned}\varepsilon = \frac{R_{\mathrm{err}}}{R_{\mathrm{key}}} &\approx \frac{g^2(1-\eta_A-\eta_B\eta_L+\eta_A\eta_B\eta_L)}{1+g^2(6-4\eta_A-4\eta_B\eta_L+3\eta_A\eta_B\eta_L)}\\ &= \frac{(1-\eta_A)(1-\eta_B\eta_L)}{2}\mu + \mathcal{O}(\mu^2).\end{aligned} \quad (9)$$

---

[4] It is taken into account that only one half of Alice's and Bob's bases coincide in average.

Clearly, if $\eta_A \to 1$ then $\varepsilon \to 0$ for all mean pair numbers μ. So Alice should have as good detectors as possible. At Bob's side the crucial limitation would probably be represented by a low line transmission η_L for real systems. If $\eta_L \ll \eta_A, \eta_B$ then $\varepsilon \approx (1-\eta_A)\,\mu/2$.

III. INFORMATION LEAKED TO EVE

Let us suppose now that Eve will try to get some information on the key only from "multi-particle" (or "multi-pair") signals in order not to make any errors in transmission. She will be allowed to use the most efficient individual attack of this kind – the photon-number-splitting (PNS) attack [12]: She substitute a lossy line by a lossless one. Then she measures the total number of photons in incoming signals. If this number is higher than one she extracts and store one photon (or more). The rest is sent to Bob by her. It is also supposed that she can control Bob's detection efficiency, so that Bob always get it. If the number of incoming photons is equal to one she either blocks the signal or passes it without other changes to Bob (in order not to decrease the data rate). After the public comparison of Alice's and Bob's bases she makes a polarization measurement on the stored photons.

The average Eve's information about sifted-key bits is

$$I_E = \sum_i r_i \left[1 + p_i \log_2 p_i + (1-p_i)\log_2(1-p_i)\right], \quad (10)$$

where r_i is a portion of bits that Eve knows with probability p_i; $\sum_i r_i = 1$. If Eve knows r per cent bits for certain and she has no idea about the others then simply $I_E = r$.

A. Weak coherent states

First let us look at the case of quantum cryptography with weak coherent states (WCS). The expected average relative length of the sifted key (in proportion to the number of all sent signals) is [10,12]

$$R_{\rm exp} = \frac{1}{2}\left[1 - \exp(-\eta_L\eta_B\mu')\right],$$

where μ' is a mean photon number in a signal state, η_B denotes Bob's detector efficiency. The average relative number of "multi-photon" signals is given by the formula

$$R_{\rm multi} = \frac{1}{2}\left[1 - (1+\mu')\exp(-\mu')\right].$$

Eve can learn all the bits stemming from these "multi-photon" signals with certainty. Thus the information leaked to Eve reads

$$I_E^{(\rm WCP)} = \begin{cases} 1 & \text{if } R_{\rm exp} \le R_{\rm multi}, \\[2ex] \dfrac{R_{\rm multi}}{R_{\rm exp}} \approx \dfrac{1}{2\eta_L\eta_B}\mu', & \text{otherwise.} \end{cases} \quad (11)$$

B. Parametric down conversion

Now, what information may leak to Eve if a parametric down-conversion (PDC) source of "single" photons is used instead of laser producing coherent states? Generated signal states (with fixed polarizations) are used for BB84 QKD-protocol in the exactly same manner as WCS [12]. The source consist of a single down-conversion crystal generating state (1) and a "yes/no" detector (with an efficiency η_A) placed in one of the two output modes. A click on this detector means that the signal state has been prepared at the other mode. The expected average relative length of the sifted key (in proportion to the number of all generated entangled states) is given by the formula

$$R_{\rm exp} = \frac{\xi^2}{2}\sum_{n=0}^{\infty} g^{2n}\left[1-(1-\eta_A)^n\right]\left[1-(1-\eta_L\eta_B)^n\right].$$

The average relative number of "multi-photon" signals reads

$$R_{\rm multi} = \frac{\xi^2}{2}\sum_{n=2}^{\infty} g^{2n}\left[1-(1-\eta_A)^n\right].$$

Again, Eve can learn all the bits carried by the "multi-photon" signals with certainty. After some straightforward calculations one can find the amount of information leaked to her:[5]

$$I_E^{(\rm PDC)} = \begin{cases} 1 & \text{if } R_{\rm exp} \le R_{\rm multi}, \\[2ex] \dfrac{R_{\rm multi}}{R_{\rm exp}} \approx \dfrac{2-\eta_A}{\eta_L\eta_B}\mu'', & \text{otherwise,} \end{cases} \quad (12)$$

were we have used the fact that in the case under consideration the mean number of pairs in each generated entangled state is $\mu'' = g^2/(1-g^2)$.

C. Entangled photons

Finally let us look at the cryptographic scheme fully based on entanglement of photon polarizations (EP); see Fig. 1. Signal states are described by Eq. (2). All the detectors are "yes/no" ones again; on Alice's side they have efficiencies η_A, on Bob's side η_B.

Here the situation is more complex. It becomes important how many photons Eve separates. However, we will confine ourselves only to the simplified situation when at most to pairs are present with a reasonable probability [see Eq. (4)]. Then Eve can separate no more than one photon and send remaining one to Bob. In contrast to

[5] It can be done exactly but for our purposes the shown approximation is good enough.

the both cases described above, now the information I_{AE} that Eve shares with Alice is *different* from the information I_{EB} that she shares with Bob. This is connected with the occurrence of errors in transmission.

The expected rate of sifted-key generation is given by Eq. (7): $R_{\rm exp} = R_{\rm key}$. A portion of two-photon signals leaving Alice's terminal – that signals that can be read by Eve applying PNS attack – is

$$R_{\rm double} = \xi^2 g^4 \left\{ \left[1 - (1-\eta_A)^2\right] + \eta_A(1-\eta_A) \right\}.$$

The first term represents contributions from states $|0,0,2,2\rangle$ and $|2,2,0,0\rangle$ the second one from $|1,1,1,1\rangle$. Only when exactly one detector clicks the bit is accepted to the key.

Calculating information it must be taken into account that now Eve does not know all measured bits with certainty. She cannot distinguish the signals stemming from states $|1,1,1,1\rangle$ from the other two-photon signals. And for these particular signals she hits Alice's bit only with probability 50 % and Bob's bit values are even always opposite to hers. Thus Eve's average information is

$$I_j^{\rm (EP)} \approx \begin{cases} f(p_j) & \text{if} \quad R_{\rm exp} \le R_{\rm double}, \\ \dfrac{R_{\rm double}}{R_{\rm exp}} f(p_j) \approx \dfrac{3-2\eta_A}{2\eta_L\eta_B} f(p_j)\,\mu, & \text{otherwise}, \end{cases} \tag{13}$$

where $j = AE, EB$ and $f(p_j) = 1 + p_j \log_2 p_j + (1-p_j)\log_2(1-p_j)$. Probabilities that Eve knows Alice's (or Bob's) bit, respectively, are given by the ratio of successful results to all results:

$$p_{AE} = \frac{5-3\eta_A}{6-4\eta_A}, \quad p_{EB} = \frac{2-\eta_A}{3-2\eta_A}.$$

Clearly, $f(p_{EB}) < f(p_{AE}) < 1$ for $\eta_A < 1$ and then also $I_{EB} < I_{AE} < 1$. Unfortunately, the fact that the maximum Eve's information [see Eq. (13)] is lower than unity (if $\eta_A < 1$) does not represent any real advantage because for $R_{\rm exp} \le R_{\rm double}$ information I_{AE} is equal to information shared by Alice and Bob, $I_{AB} = 1 + \varepsilon' \log_2 \varepsilon' + (1-\varepsilon')\log_2(1-\varepsilon')$.

Notice the other important feature of PNS eavesdropping in EP systems which is similar to "single particle" attacks: If Eve applies PNS attack by the way described above, i.e. if she tries to reproduce only the transmission rate ($R_{\rm exp}$), she *increases* the error rate. The reason is that she increases the portion of $|1,1,1,1\rangle$ contributions to the key bits. Clearly, this portion gets the following value: $R_{\rm err}^{(E)} = \xi^2 g^4 \eta_A(1-\eta_A)/2$. Thus due to eavesdropping the error rate grows to

$$\varepsilon' = \begin{cases} \dfrac{R_{\rm err}^{(E)}}{R_{\rm double}} \approx \dfrac{1-\eta_A}{6-4\eta_A}, & \text{if} \quad R_{\rm exp} \le R_{\rm double}, \\ \dfrac{R_{\rm err}^{(E)}}{R_{\rm exp}} \approx \dfrac{1-\eta_A}{4\eta_B\eta_L}\mu. & \text{otherwise}, \end{cases} \tag{14}$$

The increase of error rate can help to detect an eavesdropper what is impossible in the analogous situation (PNS attack) with WCS and PDC systems.

IV. HOW TO RESTRICT EVE'S ACTIVITY

In the previous section Eve was restricted by the demand to reproduce transmission rate (average number of sifted-key bits) only. However, it is not the only quantity which could be monitored by Bob. In all the mentioned techniques Bob can also measure the double-click rate in that events when he used a different basis than Alice. In case of EP Bob can even monitor double-click rate in situations with coincident bases (and, of course, the error rate). Clearly such Bob's activities pose other important restrictions to Eve [13]. Even more possibilities are offered by passive arrangement, when Alice and Bob do not change bases actively (see, e.g., Ref. [14]).

V. CONCLUSIONS

We discussed the effect of "multi-pair signals", that inevitably appear in any system with a parametric-down-conversion source, on the security of quantum cryptography. We have shown that there is an important difference between the quantum-cryptographic setup that uses such a source just as a "triggered source of photons" and that which employs the entanglement of pairs of generated signals directly for quantum key distribution. In the latter case there is a still nonzero error rate even if there is no eavesdropper. This is caused by the joint effect of the occurrence of "multi-pair signals" and of low detection efficiencies. However, the most important result is that in the latter setup an individual eavesdropping on "multi-pair signals" increases the error rate in the transmission.

ACKNOWLEDGMENTS

M. D. acknowledges discussions with Zachary Walton. This work has been supported under the project LN00A015 and Research Plan CEZ:J14 "Wave and Particle Optics" of the Ministry of Education of the Czech Republic and the project 19982003012 of the Czech National Security Authority.

[1] G. S. Vernam, Journal of the American Institute of Electrical Engineers **45**, 109 (1926).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[3] S. Wiesner, SIGACT News **15**, 78 (1983).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[6] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[7] D. F. Walls and G. J. Milburn, *Quantum Optics* (Spinger-Verlag, Heidelberg, 1994), p. 84.
[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[9] H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).
[10] M. Dušek, O. Haderka, and M. Hendrych, Opt. Comm. **169**, 103 (1999).
[11] N. Lütkenhaus, Phys. Rev. A. **61**, 052304 (2000).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Senders, Phys. Rev. Lett. **85**, 1330 (2000).
[13] M. Dušek, M. Jahma, N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).
[14] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).